REMARKS

STATUS OF CLAIMS

Claims 1-26 are pending.

The Examiner rejects claims 1-6 and 16-26 under 35 USC 103(a) as being unpatentable over Yasukawa (US Patent No. 5,999,622), Rhoads (US Patent No. 6,343,138), and Millsted (US Patent No. 6,263,313). Millsted is newly cited, and, thus, newly relied upon.

The Examiner rejects claims 7-15 under 35 USC 103(a) as being unpatentable over Yasukawa/Rhoads/Millsted in view of Applicants own Admission (ADA).

Page 2, item 4, of the final Office Action is the Response to Arguments.

The independent claims are 1, 25 and 26, which are rejected over Yasukawa, Rhoads, and Millsted.

Thus, claims 1-26 remain pending for reconsideration, which is respectfully requested.

No new matter has been added in this response. The foregoing rejections are hereby traversed, as follows.

CLAIM REJECTIONS

YASUKAWA

In page 3 of the final Office Action, the Examiner quotes from a claim 1 recitation prior to the October 22, 2003 Amendment, and only adds (as underlined): "However, in column 3, lines 39-52, Yasukawa discloses encrypting only some segments of the complete file. Naturally, this would entail some form of extraction process." However, as also emphasized during the interview with the Examiner on October 16, 2003, the Applicants respectfully assert it is unreasonable to characterize Yasukawa's VBT table to be similar to the digital content sample extraction of the present invention, as expressly recited in independent claims 1, 25 and 26, using claim 1 as an example, as follows.

1. (PREVIOUSLY PRESENTED) A data management method comprising:

extracting a portion of a digital content to be distributed as sample data;

preparing a substantive data unit by encrypting the digital content;

preparing a sample data unit by embedding authorization information containing information for accessing the encrypted digital content as invisible information in the extracted sample data;

preparing a synthesized data unit by synthesizing the substantive data unit and the sample data unit having the embedded authorization information; and

distributing the synthesized data unit.

Yasukawa's VBT identifies for a file stored on a disk, what and how disk sectors that store the file have been encrypted, which differs from the present invention's digital content sample extraction, because designating a disc sector of a stored file and encrypting the disc sector of the stored file is not the same as (differs from) extracting a sample of the file. In contrast to a disc sector, a file sample can be used for many purposes, including preview, but also as used in the present claimed invention for, "preparing a sample data unit by embedding authorization information containing information for accessing the encrypted digital content as invisible information in the extracted sample data" (claim 1). In other words, in Yasukawa, the segments of the complete file are disk segments (column 3, lines 45-52 and column 6, lines 30-38), and encrypting only some disk segments of the complete file is not the same as a sample of the complete file.

Further, on page 4, last paragraph, of the final Office Action, the Examiner asserts: "The combination of Yasukawa/Rhoads does not specifically disclose data samples for preview purposes," and relies on Millsted for disclosing the present invention's "extracting a portion of a digital content to be distributed as sample data" and "preparing a sample data unit by embedding authorization information containing information for accessing the encrypted digital content as invisible information in the extracted sample data" (claim 1).

Therefore, except the for the foregoing comments regarding Yasukawa's VBT, the previous arguments regarding the present claimed invention's patentable differences over Yasukawa and Rhoads are not repeated here from the previous Amendment of October 22, 2003 and still apply. The present claimed invention's patetable differences over the newly relied

upon Millsted, which is relied upon to reject the present claimed invention's sample data extraction and embedding authorization information therein, is discussed below.

MILLSTED

Millsted discloses a method of automatically selecting processing parameters for encoding digital content. Metadata containing the genre of the digital content, receiving the compression level selected for encoding the digital content is received. An algorithm selected for encoding the digital content is received. Abstract.

THE PRESENT CLAIMED INVENTION'S USE OF A DIGITAL CONTENT SAMPLE

Regarding the present claimed invention's use of a digital content sample, Millsted in column 81, lines 45-55, which is relied upon by the Examiner, discloses a user previewing sample digital clips as part of on-line digital content shopping experience. However, the present claimed invention is using a sample of digital content to also embed authorization information therein, which differs from Millsted providing samples only for user preview during online shopping. The independent claims 1, 25 and 26 are not directed to digital content preview samples as in online shopping per se, but the independent claims recite the idea of using extracted digital content samples as part of secure data distribution management, so that although a digital content sample can be a preview sample, the claims are directed to using such a sample as part of secure data distribution management, which is not disclosed or suggested by Millsted as well as Yasukawa's VBT and Rhoads.

PRESENT CLAIMED INVENTION'S DIGITAL CONTENT SAMPLE EXTRACTION AND PREVIEWING

Regarding the present claimed invention's digital content sample extraction and previewing, Millsted in column 75, lines 9-21, which is relied upon by the Examiner, discloses a Metadata 620. Millsted, in column 12, lines 5-11, discloses that the Metadata 620 is data related to the Content 113 and in this embodiment does not include the Content 113 itself, so as an example, metadata for a song may be a song title or song credits, but not the sound recording of the song, and the Content 113 would contain the sound recording. Millsted, in column 12, lines 33-44, discloses that the encrypted Content 113, digital content-related data or metadata, and encrypted keys are packed in Secure Containers (SCs), and because the Content 113 and the Keys are encrypted and packed in SCs, Electronic Digital Content Stores 103 or any other hosting agent cannot directly access decrypted content 113 without clearance from the Clearinghouses. Because Millsted packs metadata in a Secure Container (SC), in column 75, lines 9-21, which is relied upon by the Examiner, Millsted discloses metadata extraction from the

SC for viewing.

First, Millsted's extraction in column 75, lines 9-21 is directed to extracting metadata from a Secure Container, and does not disclose the present invention's, "extracting a portion of a digital content to be distributed as sample data." Second, although Millsted's metadata can be a sample of a digital content, Millsted only uses the metadata for preview purposes and does not use the metadata for secure distribution management purposes. In particular, Millsted in column 12, lines 34-35, discloses that encrypted keys are packed in SCs, suggesting that the metadata is provided in the SCs solely for preview purposes and not like the present claimed invention's secure distribution management. In other words, Millsted does not provide the present claimed invention's, "preparing a sample data unit *by embedding authorization information* containing information for accessing the encrypted digital content as invisible information *in the extracted sample data*" (claim 1, emphasis added).

Further, Millsted, in column 10, lines 24-33, discloses that the digital code is either watermarked in the Content or just kept as part of the usage conditions associated with the Content 113. See also, Millsted, column 23, lines 57-60; column 31, lines 51-53. Further, Millsted, in column 75, lines 2-4, discloses the Metadata SCs 620 can contain encrypted free promotional content, however, Millsted fails to disclose or suggest the present invention's, "preparing a sample data unit *by embedding authorization information* containing information for accessing the encrypted digital content as invisible information *in the extracted sample data*" (claim 1). In other words, Millsted does not do anything with the metadata that relates to security of the digital content, or Millsted does not watermark the metadata. In contrast to Millsted, the present invention provides, "preparing a sample data unit by *embedding authorization information* containing information for accessing the encrypted digital content as invisible information *in the extracted sample data*" (claim 1).

Further, the Examiner relies on Millsted, column 64, line 61 to column 65, line 18, for watermarking. However, in column 64, line 61 to column 65, line 18 as well as in column 12, lines 21-22, Millsted expressly discloses: "A Watermarking Tool is used to hide data in the Content 113," such that Millsted does not perform the present invention's, "preparing a sample data unit by *embedding authorization information* containing information for accessing the encrypted digital content as invisible information *in the extracted sample data*" (claim 1). In other words, Millsted does not watermark the metadata.

The Examiner also relies on Millsted, column 2, line 52 to column 3, line 4, which discloses two ways of electronic digital content distribution, one way uses a secure network, and

another way uses an unsecured network but with the digital content secured, and a need to protect the digital content after delivery to consumers and businesses. However, Millsted does not disclose or suggest the present invention's claimed secure content distribution management using extracted digital samples of the content as part of the secure content distribution management, having a benefit of an efficient/simple, but secure, digital content delivery to consumers and business.

YASUKAWA, RHOADS AND MILLSTED

Yasukawa, Rhoads, and Millsted, do not disclose, suggest, or contemplate, the claimed invention as recited in independent claims 1, 25 and 26, which provides:

(1) extract a portion of digital content as a sample,

(2) encrypt the digital content,

(3) embed invisible authorization information for accessing the encrypted digital content in the sample, and

(4) synthesize the sample with the encrypted digital content, and

(5) distribute the synthesized data.

Benefits of the claimed invention, which are not achieved or contemplated by Yasukawa, Rhoads, and Millsted, are as follows:

(1) Allowing a provider to efficiently manage distribution of the encrypted complete data and its non-encrypted sample with one file and allowing the user not to manage a separate key for the encrypted complete data and its non-encrypted sample. In particular, merits of the present invention for a user are as follows: because of the present invention, for example, two kinds of image data, (1) a non-encrypted sample image, and (2) an encrypted substantive image of the non-encrypted sample image (i.e., an encrypted complete image as licensed), are efficiently stored in a single file (i.e., the "synthesized data unit"), allowing a provider to efficiently manage with one file distribution the encrypted complete data and its non-encrypted sample, and allowing the user not to manage a separate key for the encrypted complete data and its non-encrypted sample.

(2) Merits of the present invention for a content provider/center are as follows: A content provider can manage both an accessible sample image and a protected substantive image (the complete image as licensed) in only one file (i.e., the "synthesized data"). Accordingly, management and administration on a server becomes simpler. In one conventional

way, as also disclosed in Millsted in column 12, lines 33-44 and column 18, line 1 to column 19, line 10, when the user desires to license the encrypted complete image, authorization information has to be obtained from a Clearinghouse. See also, Millsted, column 25, line 64, to column 26, line 6. In particular, Millsted, in column 12, lines 33-44, discloses that the encrypted Content 113, digital content-related data or metadata, and encrypted keys are packed in Secure Containers (SCs), and because the Content 113 and the Keys are encrypted and packed in SCs, Electronic Digital Content Stores 103 or any other hosting agent cannot directly access decrypted content 113 without clearance from the Clearinghouses. In the other way disclosed by Millsted, in column 10, lines 24-33, the digital code is either watermarked in the Content or just kept as part of the usage conditions associated with the Content 113. See also, Millsted, column 23, lines 57-60; column 31, lines 51-53. Further, Millsted, in column 75, lines 2-4, discloses the Metadata SCs 620 can contain encrypted free promotional content, however, Millsted fails to disclose or suggest the present invention's, "preparing a sample data unit *by embedding authorization information* containing information for accessing the encrypted digital content as invisible information *in the extracted sample data*" (claim 1). In other words, Millsted does not do anything with the metadata that relates to security of the digital content, or Millsted does not watermark the metadata.

In contrast to Millsted, in the present invention authorization information is retrieved from the sample image and the user does not have to interface with a Clearinghouse to decrypt the encrypted digital content. Therefore, a possibility that a license file is deleted inadvertently is reduced, because both the images and the license for using the images are included in one file (i.e., the "sample data" with invisible authorization information and the encrypted complete data are both included in the synthesized data unit). More particularly, conventionally, two files are provided, one for the images and one for the license, and, accordingly, damages caused by deleting a license file is significant, and data storage management is less efficient by using two files.

CONCLUSION

In view of the remarks, withdrawal of the rejections of claims 1-26 and allowance of claim 1-26 is respectfully requested.

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Respectfully submitted,
STAAS & HALSEY LLP

Date: May 13, 2004

By: _____
Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501